Available online at www.sciencedirect.com
SCIENCE DIRECT®
Discrete Mathematics 305 (2005) 55–73
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Extensions of the Critical Theorem☆

Thomas Britz

Department of Mathematics and Statistics, University of Victoria, Victoria, BC, Canada V8W 3P4

Received 1 October 2005; accepted 3 October 2005

Abstract

The Critical Theorem, due to Henry Crapo and Gian-Carlo Rota, has previously been extended or generalised in a number of different ways. The main result of the present paper is a general form of the Critical Theorem that encompasses many of these results. Applications include generalisations of a theorem by Curtis Greene that describes how the weight enumerator of a linear code is determined by the Tutte polynomial of the associated vector matroid, as well as generalisations of the MacWilliams identity for linear codes.

Keywords: The Critical Theorem; Matroid; Linear code; Support

1. Introduction

In his seminal paper [30] on matroid theory, Hassler Whitney drew attention to the problem of characterising matroids that are representable over a given field, a problem that has dominated matroid theory ever since. Whitney took steps towards solving this problem by proving that a matroid is binary if and only if every symmetric difference of circuits is a disjoint union of circuits. Using this characterisation, Tutte [27] further proved that a matroid is binary if and only if it does not contain the minor $U_{2,4}$. Through the work of Tutte and of many others, such forbidden minor characterisations have proved to be a quite successful approach. See [21] for a partial overview of these results.

The forbidden minor characterisations have been the only results to offer significant partial solutions to the problem of characterising matroid representability. Although Crapo

☆ Part of this research was conducted at the University of Aarhus and at Queen Mary, University of London.

E-mail address: sonofnob@gmail.com.

0012-365X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2005.10.002

and Rota did not primarily perceive it as such, their Critical Theorem [10] from 1970 is an important result on matroid representability. This is most obvious when the problem of matroid representability is viewed from the viewpoint that is more or less explicitly presented in Whitney's paper: rather than investigate whether a given matroid represents some linear code over a given field, one might wish to describe the relation between a given linear code and its vector matroid. Equivalently, one might describe the extent and nature of the code structure that may be retrieved from the vector matroid. It is in this setting that the Critical Theorem has found its greatest application, for it describes in detail the codeword supports of the given code in terms of its matroid properties. In 1971, Dowling [11] generalised the Critical Theorem and in 1976, Greene [13] presented a surprising coding theoretical application of the Critical Theorem. However, it is not until recently that the Critical Theorem has gained proper recognition, in [3,5,16] among other places.

The main result of this article is a generalisation of the Critical Theorem that makes clear, in detail, the extent and nature of those structural properties of a linear code that are determined by the associated vector matroid.

Notation and definitions are presented in Section 2. In Section 3, the main result is presented, and applications of this result to code enumerators appear in Section 4. The results thus obtained generalise Greene [13, Corollary 4.5] by describing how the rank generating function of the vector matroid of a linear code determines the weight enumerators of the code. Following Greene's example, these generalisations are employed, in Section 5, to prove a number of generalisations of the MacWilliams identity [18] that relates the weight enumerator of a linear code to that of its dual. Some remarks conclude the article in Section 6.

The results of this paper were presented at the conference on the Graph Theory of Brian Alspach, Simon Fraser University, May 25–29, 2003.

2. The vector matroid of a linear code

Let $\mathbb{F}$ be a field and let E denote a set of $n \geqslant 1$ distinct elements. A *linear code* on E over $\mathbb{F}$ is a subspace of the vector space $\mathbb{F}^E$, i.e., a vector space over $\mathbb{F}$ with coordinates indexed by the elements of E. The elements of a linear code are called *codewords*. Throughout this paper, the notation $\{f_e\}_X$ denotes any multiset $\{f_e : e \in X\}$ whose elements f_e are labelled by the elements $e \in X$. If $v = \{v_e\}_E$ is a codeword of $\mathbb{F}^E$, then let the set

$$S(v) = \{e \in E : v_e \neq 0\}$$

denote the *support* of v, and let

$$w(v) = |S(v)|$$

denote the *(Hamming) weight* of v. In general, the support of a set of vectors $V \subseteq \mathbb{F}^E$ is given by

$$S(V) = \bigcup_{v \in V} S(v).$$

Associate to each element $e \in E$ a variable z_e, and set $\mathbf{z} := \{z_e\}_E$.

We assume a basic knowledge of matroid theory. For excellent introductions to this topic, see [21,29]. Let G be a generator matrix for a linear code $C \subseteq \mathbb{F}^E$. The vector matroid $M_C = M[G]$ is the matroid on E whose independent sets are the linearly independent columns of G. The code C and the matroid M_C are quite closely related. For instance, it is not hard to show that M_C is independent of the chosen generator matrix G, and that the dual matroid corresponds to the dual code: $(M_C)^* = M_{C^\perp}$. However, the code C contains more information than the matroid M_C. Indeed, a matroid may be (isomorphic to) the vector matroid of several linear codes that are not monomially equivalent, even over the same field. The following result (see [21, Theorem 9.2.4] and [28, 1.21]) characterises M_C in terms of the codeword supports of C.

Theorem 1. *For each linear code $C \subseteq \mathbb{F}^E$, the cocircuits of M_C are precisely the minimal nonempty codeword supports of C.*

Theorem 1 describes the relationship between supports and cocircuits and indicates how the cocircuits of the matroid M_C may be obtained from the set of codeword supports of the code C. However, it is not clear from this theorem that the set of supports may be recovered from the matroid. For more information on minimal nonempty codeword supports from a purely coding-theoretical viewpoint, see [2] for instance.

Throughout the following, let q be a prime power and let $\mathbb{F}_q$ be the finite field consisting of q elements. The *characteristic polynomial* $P(M; \lambda)$ of a matroid M on the set E may be defined by the sum

$$P(M; \lambda) = \sum_{X \subseteq E} (-1)^{|X|} \lambda^{\rho(E)-\rho(X)},$$

where ρ denotes the rank function of M.

Theorem 1 in Crapo and Rota [10, Chapter 16], widely known as the Critical Theorem, asserts that the matroid M_C not only determines the set of codeword supports of the code C, it even determines the multiset of these supports. The theorem has been restated and extended slightly here, in a manner similar to that of Greene [13, Proposition 3.2]. For any matroid M on E, $M.X$ denotes the contraction $M/(E - X)$.

Theorem 2 (*The Critical Theorem*). *Let $X \subseteq E$ and $m \in \mathbb{N}$ be given. For each linear code $C \subseteq \mathbb{F}_q^E$, the number of ordered m-tuples $V = (v_1, \ldots, v_m)$ of codewords $v_1, \ldots, v_m \in C$ with $S(V) = X$ is $p(M_C.X; q^m)$.*

Note in particular that X is the support of some codeword of C if and only if $p(M_C.X; q) > 0$. The special case of the Critical Theorem in which $m = 1$ was proved independently by Brualdi et al. [8]. It is not hard to show that this case actually implies all other cases. Generalisations of the Critical Theorem may be found in [3,6,11,16]. A new generalisation appears in Section 3. It extends several of the previous generalisations and gives rise to many others.

The *weight enumerator* $A_C(z)$ of a linear code $C \subseteq \mathbb{F}_q^E$ is the sum

$$A_C(z) = \sum_{i=0}^{n} A_i z^i,$$

where $A_i = |\{v \in C : w(v) = i\}|$. Greene [13] showed that it is often sufficient to regard only part of the information contained in the matroid in order to describe some property of the code. In particular, Greene proved that the weight enumerator $A_C(z)$ of the code C is determined by the *rank generating function* of the matroid M_C,

$$R(\mathscr{M}_C; x, y) = \sum_{X \subseteq E} x^{\rho(E)-\rho(X)} y^{|X|-\rho(X)}.$$

Theorem 3 (*Greene [13]*). *If $C \subseteq \mathbb{F}_q^E$ is a linear code of dimension k, then*

$$A_C(z) = (1-z)^k z^{n-k} R\left(\mathscr{M}_C; \frac{qz}{1-z}, \frac{1-z}{z}\right).$$

As an application of Theorem 3, Greene presented a simple proof of the MacWilliams identity [18] (see Theorem 21) that relates the weight enumerator of a linear code C to that of the dual code $C^\perp$. Generalisations of these results are presented in [4,5] as well as in Section 4.

In order to generalise Theorem 3, it is helpful to first generalise the rank generating function. If g and h are functions on $\mathbb{Q}(X)$, the ring of rational forms over the rational numbers $\mathbb{Q}$, then define a *generalised rank generating function*

$$R_{g,h}(M; x, y, \mathbf{z}) = \sum_{X \subseteq E} x^{\rho(E)-\rho(X)} y^{|X|-\rho(X)} \left(\prod_{e \in X} g(z_e)\right) \prod_{f \in E-X} h(z_f).$$

Note that the rank generating function is obtained by letting g and h be the identity function and setting $z_e = 1$ for all $e \in E$. In the following, g and h will be taken to be the functions $x \mapsto 1-x$ and $x \mapsto x$, respectively. For information on generalised rank generating functions and closely related polynomials, see [5,25,26,32]. The following proposition will prove useful in Section 5.

Proposition 4 (*Britz [5]*). $R_{g,h}(M^*; x, y, \mathbf{z}) = R_{h,g}(M; y, x, \mathbf{z})$.

3. Extensions of the Critical Theorem

In this section, we will demonstrate how the Critical Theorem may be generalised in a simple manner. For this purpose, some technical definitions must be presented. A *structure of order* 1 on a multiset X is a finite multiset ς consisting of copies of some elements from X, either unordered or totally ordered. The *ground set* of such a structure ς is the set

$$G(\varsigma) = \{x \mid x \in \varsigma\}.$$

For $m = 2, 3, \ldots$, recursively define a *structure of order* $m > 1$ on a multiset X to be a finite multiset ς consisting of copies of some structures $\varsigma_1, \ldots, \varsigma_t$ (for some $t \in \mathbb{N}$) that are each of order at most $m-1$ on X, where this collection of copies is either unordered or totally ordered. The *ground set* of ς is the union

$$G(\varsigma) = G(\varsigma_1) \cup \cdots \cup G(\varsigma_t).$$

For some fixed $s \in \mathbb{N}$, let $q_1, \ldots, q_s$ be not necessarily distinct prime powers and, for each $i = 1, \ldots, s$, let $\mathbb{F}_{q_i}$ denote the finite field consisting of q_i elements. For each multiset $\{C_1, \ldots, C_s\}$ of linear codes $C_i \subseteq \mathbb{F}_{q_i}^E$ $(i = 1, \ldots, s)$ and each structure ς on the multiset $C_1 \cup \cdots \cup C_s$, the *support* of ς is the set

$$S(\varsigma) = \bigcup_{v \in G(\varsigma)} S(v).$$

A *code structure family* over the fields $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_s}$ is a family $\mathscr{S}$ each member of which is a structure on the multiset of vectors $C_1' \cup \cdots \cup C_s'$ in some linear codes $C_1', \ldots, C_s'$ over $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_s}$, respectively, with the following property:

(1) For each structure $\varsigma \in \mathscr{S}$ on the multiset of vectors $C_1 \cup \cdots \cup C_s$ in some linear codes $C_1 \subseteq \mathbb{F}_{q_1}^E, \ldots, C_s \subseteq \mathbb{F}_{q_s}^E$ with common coordinates E and a common vector matroid $M = M_{C_1} = \cdots = M_{C_s}$, and for each subset $X \subseteq E$, the number of structures $\varsigma' \in \mathscr{S}$ on the multiset of vectors in the codes $C_1/X, \ldots, C_s/X$ is equal to the number of structures $\varsigma'' \in \mathscr{S}$ on the multiset $C_1 \cup \cdots \cup C_s$ with $S(\varsigma'') \cap X = \emptyset$.

A code structure family $\mathscr{S}$ is said to be *invariant* if, whenever $\mathscr{S}$ contains a structure ς on a multiset $C_1 \cup \cdots \cup C_s$, where $C_1 \subseteq \mathbb{F}_{q_1}^E, \ldots, C_s \subseteq \mathbb{F}_{q_s}^E$ are linear codes with a common vector matroid $M = M_{C_1} = \cdots = M_{C_s}$ and thus in particular a common dimension k, the number of structures in $\mathscr{S}$ on the multiset $C_1 \cup \cdots \cup C_s$ is determined uniquely by the integers $q_1, \ldots, q_s$, and k. Denote this number as

$$a(\mathscr{S}; q_1, \ldots, q_s, k).$$

For all integers $a, b, k, \lambda, r \geqslant 0$, define

$$[a]_b := \prod_{i=0}^{b-1} (q^a - q^i), \quad \begin{bmatrix} k \\ r \end{bmatrix} := \frac{[k]_r}{[r]_r} \quad \text{and} \quad \begin{bmatrix} k \\ r \end{bmatrix}_\lambda := \prod_{i=0}^{r-1} \left(\frac{\lambda^k - \lambda^i}{\lambda^r - \lambda^i} \right).$$

Note that $\begin{bmatrix} k \\ r \end{bmatrix} = \begin{bmatrix} k \\ r \end{bmatrix}_q$ is the number of distinct r-dimensional subspaces of a k-dimensional vector space over $\mathbb{F}_q$.

Examples of invariant code structure families on a single linear code $C \subseteq \mathbb{F}_q^E$ (i.e., $s = 1$) are listed in Table 1. Most of the expressions $a(\mathscr{S}; q, k)$ are obtained by simple counting arguments (see [1,17,24] for details). The last two families in Table 1 consist of structures of order 2, whereas the preceding families consist of structures of order 1. Another example of an invariant family (consisting of structures of order 1) is the code structure family

Table 1
Some invariant code structure families on linear codes over $\mathbb{F}_q$

Code structure family $\mathscr{S}$	$a(\mathscr{S}; q, k)$
Vectors	q^k
Zero vectors	1
Non-zero vectors	$q^k - 1$
m-tuples of vectors	q^{km}
m-tuples of distinct vectors	$(q^k)_m$
Unordered multisets of m vectors	$\binom{q^k+m-1}{m}$
Unordered sets of m distinct vectors	$\binom{q^k}{m}$
r-dimensional vector spaces	$\begin{bmatrix} k \\ r \end{bmatrix}$
Unordered sets of m distinct r-dimensional vector spaces	$\binom{\begin{bmatrix} k \\ r \end{bmatrix}}{m}$
Ordered partitions of all vectors into q-sized blocks	$\frac{(q^k)!}{(q!)^k}$

Table 2
A few code structure families on linear codes $C_1 \subseteq \mathbb{F}_{q_1}^E, \ldots, C_s \subseteq \mathbb{F}_{q_s}^E$

Code structure family $\mathscr{S}$	$a(\mathscr{S}; q_1, \ldots, q_s, k)$
Vectors contained in the multiset $C_1 \cup \cdots \cup C_s$	$q_1^k + \cdots + q_s^k$
Zero vectors contained in the multiset $C_1 \cup \cdots \cup C_s$	s
Non-zero vectors contained in the multiset $C_1 \cup \cdots \cup C_s$	$q_1^k + \cdots + q_s^k - s$
s-tuples of vectors $(v_1, \ldots, v_s)$ where $v_i \in C_i$ $(i = 1, \ldots, s)$	$q_1^k \cdots q_s^k$
s-tuples $(T_1, \ldots, T_s)$ of m_i-tuples $T_i \subseteq C_i$ $(i = 1, \ldots, s)$	$q_1^{km_1} \cdots q_s^{km_s}$
$s \times m$ matrices (v_{ij}) where $v_{i1}, \ldots, v_{im} \in C_i$ are distinct	$(q_1^k)_m \cdots (q_s^k)_m$

$\mathscr{S}$ of ordered m-tuples of vectors whose span has dimension r (see [12, Theorem 2] and [17, p. 303]):

$$a(\mathscr{S}; q, k) = \begin{bmatrix} k \\ r \end{bmatrix} \sum_{i=0}^{r} (-1)^{r-i} \begin{bmatrix} r \\ i \end{bmatrix} q^{mi+\binom{r-i}{2}} = \begin{bmatrix} k \\ r \end{bmatrix} [m]_r.$$

A more exotic example of an invariant family (of structures of order 3) is the code structure family $\mathscr{S}$ of pairs consisting of a non-zero vector and an m-tuple of r-dimensional vector spaces:

$$a(\mathscr{S}; q, k) = (q^k - 1) \begin{bmatrix} k \\ r \end{bmatrix}^m.$$

Table 2 presents only a few examples of invariant code structure families but indicates how many other invariant code structure families may be defined. To illustrate, consider the code structure family $\mathscr{S}$ consisting of ordered pairs (C', V), where C' is an r-dimensional subspace of a fixed k-dimensional linear code over $\mathbb{F}_{q_1}$, and V is an unordered multiset of

m vectors of a fixed k-dimensional linear code over $\mathbb{F}_{q_2}$. Then $\mathscr{S}$ is invariant, and

$$a(\mathscr{S}; q_1, q_2, k) = \begin{bmatrix} k \\ r \end{bmatrix}_{q_1} \begin{pmatrix} q_2^k + m - 1 \\ m \end{pmatrix}.$$

For the rest of this section, let $C_1 \subseteq \mathbb{F}_{q_1}^E, \ldots, C_s \subseteq \mathbb{F}_{q_s}^E$ be linear codes with a common vector matroid $M = M_{C_1} = \cdots = M_{C_s}$ over a nonempty, finite set E, and let $\mathscr{S}$ be an invariant code structure family over $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_s}$. Let ρ denote the rank function of M. The main result of this section is the following generalisation of the Critical Theorem.

Theorem 5. *For each $X \subseteq E$, the number of structures $\varsigma \in \mathscr{S}$ on the multiset $C_1 \cup \ldots \cup C_s$ with $S(\varsigma) = X$ is*

$$\sum_{Y \subseteq X} (-1)^{|Y|} a(\mathscr{S}; q_1, \ldots, q_s, \rho(E) - \rho(Y \cup (E - X))).$$

Proof. Consider first the case $X = E$. For each $e \in X$, let N_e be the property that the support $S(\varsigma)$ of a structure $\varsigma \in \mathscr{S}$ on the multiset $C_1 \cup \cdots \cup C_s$ does not contain e. We wish to find the number of structures $\varsigma \in \mathscr{S}$ that do not satisfy any of these properties N_e. Let $Y \subseteq X$. By definition, the number of structures $\varsigma \in \mathscr{S}$ whose support $S(\varsigma)$ does not contain any element of Y is equal to the number of structures $\varsigma' \in \mathscr{S}$ on the multiset $(C_1/Y) \cup \cdots \cup (C_s/Y)$. By the invariance of $\mathscr{S}$ and the identity $\dim C_i/Y = \rho(X) - \rho(Y)$ $(i = 1, \ldots, s)$, this number is $a(\mathscr{S}; q_1, \ldots, q_s, \rho(X) - \rho(Y))$. It follows from the Inclusion–Exclusion Principle that the number of structures $\varsigma \in \mathscr{S}$ with $S(\varsigma) = X$ is

$$\sum_{Y \subseteq X} (-1)^{|Y|} a(\mathscr{S}; q_1, \ldots, q_s, \rho(X) - \rho(Y)).$$

For the general case $X \subseteq E$, replace the matroid M by the contraction $M.X$ in the proof above and apply the identity

$$\rho_{M.X}(X) - \rho_{M.X}(Y) = \rho(E) - \rho(Y \cup (E - X)). \qquad \square$$

To obtain the Critical Theorem from Theorem 5, let $\mathscr{S}$ be the code structure family of ordered m-tuples of vectors over $\mathbb{F}_q$. Since $a(\mathscr{S}; q, k) = q^{mk}$, Theorem 5 states that the number of ordered m-tuples $\varsigma = (v_1, \ldots, v_m)$ of codewords $v_1, \ldots, v_m \in C$ with $S(\varsigma) = X$ is

$$\sum_{Y \subseteq X} (-1)^{|Y|} (q^m)^{\rho(E) - \rho(Y \cup (E-X))} = p(M_C.X; q^m).$$

Another special case of Theorem 5 is the following result due to Kung (see [16, Theorem 4.3]).

Corollary 6. *Let $X \subseteq E$. The number of s-tuples $(v_1, \ldots, v_s)$ of codewords $v_i \in C_i$ $(i = 1, \ldots, s)$ with $S(v_1) \cup \cdots \cup S(v_s) = X$ is $P(M.X; q_1 \cdots q_s)$.*

Proof. Let $\mathscr{S}$ be the code structure family over $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_s}$ consisting of ordered m-tuples $(v_1, \ldots, v_m)$, where for each $i = 1, \ldots, s$, v_i is a vector in a linear code C_i' over

$\mathbb{F}_{q_i}$. Then $a(\mathscr{S}; q_1, \ldots, q_m, k) = q_1^k \cdots q_m^k = (q_1 \cdots q_m)^k$, and the corollary follows from Theorem 5. □

The Critical Theorem follows from Corollary 6 by setting $C_1 = \cdots = C_m = C$. The following higher-dimensional analogue of Corollary 6 is obtained by letting $\mathscr{S}$ be the code structure family over $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_s}$ consisting of s-tuples $(C_1', \ldots, C_s')$ of subspaces $C_i' \subseteq C_i$ with dimension r_i $(i = 1, \ldots, s)$, and applying Theorem 5.

Corollary 7. *Let $X \subseteq E$. The number of s-tuples $(C_1', \ldots, C_s')$ of subspaces $C_i' \subseteq C_i$ with dimension r_i $(i = 1, \ldots, s)$ such that $S(C_1') \cup \cdots \cup S(C_s') = X$ is*

$$\sum_{Y \subseteq X} (-1)^{|Y|} \prod_{i=1}^{s} \begin{bmatrix} \rho(E) - \rho(Y \cup (E - X)) \\ r_i \end{bmatrix}_{q_i}.$$

The matroid $M = M_{C_1} = \cdots = M_{C_s}$ determines its contractions and is in turn determined by the minimal nonempty codeword supports of any of the codes $C_1, \ldots, C_s$, by Theorem 1. Therefore, Theorem 5 implies that the minimal nonempty codeword supports of any code C_i determine, together with the numbers $q_1, \ldots, q_s$, not only the multiset of codeword supports of each code C_i $(i = 1, \ldots, s)$ but also many other and more subtle properties of these codes. Let us state this more explicitly.

Theorem 8. *For each subset $X \subseteq E$, the number N of structures $\varsigma \in \mathscr{S}$ with $S(\varsigma) = X$ is uniquely determined by the numbers $q_1, \ldots, q_s$ and by the set of minimal nonempty codeword supports of any code $C' \in \{C_1, \ldots, C_s\}$. Indeed,*

$$N = \sum_{Y \subseteq X} (-1)^{|Y|} a(\mathscr{S}; q_1, \ldots, q_s, c(Y \cup (E - X))),$$

where $c(T)$ is the maximal integer m for which the set of minimal nonempty codeword supports of C' contains m sets $P_1, \ldots, P_m \subseteq E - T$ so that no set P_j is contained in the union of the other $m - 1$ sets.

Proof. By well-known identities (see [9, p. 306] for instance), $\rho(E) - \rho(T)$ is the maximal integer m for which the matroid M contains m cocircuits $P_1, \ldots, P_m \subseteq E - T$ such that no cocircuit P_j is contained in the union of the other $m - 1$ cocircuits. By Theorem 1, $c(Y \cup (E - X)) = \rho(E) - \rho(Y \cup (E - X))$. Theorem 5 concludes the proof. □

Theorems 5 and 8 generalise the Critical Theorem and describe in detail the extent and nature of the information regarding the code support structure that is obtainable from the associated vector matroid. It is therefore natural to wonder whether these theorems are in some sense optimal.

Conjecture 9. All general code properties that are determined by the vector matroids associated to the code may be determined by using Theorems 5 and 8. In other words, each of these properties may be represented by some invariant code structure family.

Properties of a code C that are not determined by its vector matroid M_C include the covering radius of C (see [7] for more details).

4. Code enumerators and the rank generating function

For $i = 1, \ldots, s$, let $C_i \subseteq \mathbb{F}_{q_i}^E$ be a linear code such that $M = M_{C_1} = \cdots = M_{C_s}$, and let $\mathscr{S}$ be an invariant code structure family over the fields $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_s}$. Set $k := \rho(M)$ and note that $k = \dim C_i$ $(i = 1, \ldots, s)$. For $\mathbf{C} = (C_1, \ldots, C_s)$, define the *$\mathscr{S}$-support enumerator*

$$A_{\mathbf{C}}^{\mathscr{S}}(\mathbf{z}) = \sum_{X \subseteq E} a_X^{\mathscr{S}} \prod_{e \in X} z_e$$

and the *$\mathscr{S}$-weight enumerator*

$$A_{\mathbf{C}}^{\mathscr{S}}(z) = \sum_{i=0}^{n} a_i^{\mathscr{S}} z^i = \sum_{X \subseteq E} a_X^{\mathscr{S}} z^{|X|},$$

where $a_X^{\mathscr{S}}$ and $a_i^{\mathscr{S}}$ denote the number of structures $\varsigma \in \mathscr{S}$ on the multiset $C_1 \cup \cdots \cup C_s$ that satisfy $S(\varsigma) = X$ and $|S(\varsigma)| = i$, respectively. If $\mathbf{C}$ consists of a single linear code $C \subseteq \mathbb{F}_q^E$, then $A_{\mathbf{C}}^{\mathscr{S}}(\mathbf{z})$ and $A_{\mathbf{C}}^{\mathscr{S}}(z)$ will be written as

$$A_C^{\mathscr{S}}(\mathbf{z}) \quad \text{and} \quad A_C^{\mathscr{S}}(z),$$

respectively. By Theorem 5,

$$A_{\mathbf{C}}^{\mathscr{S}}(\mathbf{z}) = \sum_{X \subseteq E} \sum_{Y \subseteq X} (-1)^{|Y|} a(\mathscr{S}; q_1, \ldots, q_s, \rho(E) - \rho(Y \cup (E - X))) \prod_{e \in X} z_e.$$

By substituting $X \mapsto Y \cup (E - X)$ in the first sum,

$$A_{\mathbf{C}}^{\mathscr{S}}(\mathbf{z}) = \sum_{X \subseteq E} a(\mathscr{S}; q_1, \ldots, q_s, \rho(E) - \rho(X)) \left(\sum_{Y \subseteq X} (-1)^{|Y|} \prod_{e \in Y} z_e \right) \prod_{f \in E - X} z_f.$$

Hence,

Lemma 10.

$$A_{\mathbf{C}}^{\mathscr{S}}(\mathbf{z}) = \sum\nolimits_{X \subseteq E} a(\mathscr{S}; q_1, \ldots, q_s, \rho(E) - \rho(X)) \left(\prod\nolimits_{e \in X} (1 - z_e) \right) \prod\nolimits_{f \in E - X} z_f.$$

Corollary 11.

$$\begin{aligned} A_{\mathbf{C}}^{\mathscr{S}}(z) &= \sum_{X \subseteq E} a(\rho(E) - \rho(X))(1 - z)^{|X|} z^{n - |X|} \\ &= (1 - z)^k z^{n-k} \sum_{X \subseteq E} a(\rho(E) - \rho(X)) \left(\frac{z}{1 - z} \right)^{\rho(E) - \rho(X)} \left(\frac{1 - z}{z} \right)^{|X| - \rho(X)}, \end{aligned}$$

where the abbreviated notation $a(k) = a(\mathscr{S}; q_1, \ldots, q_s, k)$ has been used.

If the function $a(\mathscr{S}; q_1, \ldots, q_s, k)$ is of the form $\sum_{i \in I} a_i q_1^{b_{i1}k} \cdots q_s^{b_{is}k}$ where the coefficients a_i, b_{ij} do not depend on k, then the expressions in Lemma 10 and Corollary 11 may be expressed as linear combinations of evaluations of the generalised rank generating function $R_{1-x,x}(M_C; \lambda, 1, \mathbf{z})$ and the rank generating function $R(M_C; \lambda, \mu)$, respectively.

This describes a general method whereby we may generalise Theorem 3. This method is described in greater detail in Theorem 13. Let us first, however, illustrate the method by the following example in which the s-tuple of linear codes consists merely of a single k-dimensional linear code over $\mathbb{F}_q$ (i.e., $s = 1$).

Example 12. If $\mathscr{S}$ is the code structure family consisting simply of all vectors, then $a(\mathscr{S}; q, k) = q^k$. Corollary 11 provides a quick proof of Theorem 3:

$$\begin{aligned} A(z) = A_{\mathbf{C}}^{\mathscr{S}}(z) &= (1-z)^k z^{n-k} \sum_{X \subseteq E} q^{\rho(E)-\rho(X)} \left(\frac{z}{1-z}\right)^{\rho(E)-\rho(X)} \left(\frac{1-z}{z}\right)^{|X|-\rho(X)} \\ &= (1-z)^k z^{n-k} R\left(\mathscr{M}_C; \frac{qz}{1-z}, \frac{1-z}{z}\right). \end{aligned}$$

The next result follows immediately from Lemma 10 and Corollary 11.

Theorem 13. *Suppose that $a(\mathscr{S}; q_1, \ldots, q_s, k)$ is of the form $\sum_{i \in I} a_i \prod_{j=1}^{s} q_j^{b_{ij}k}$ in which the coefficients a_i, b_{ij} are independent of k. Then*

$$A_{\mathbf{C}}^{\mathscr{S}}(\mathbf{z}) = \sum_{i \in I} a_i R_{1-x,x}(M_C; q_1^{b_{i1}} \cdots q_s^{b_{is}}, 1, \mathbf{z})$$

and

$$A_{\mathbf{C}}^{\mathscr{S}}(z) = (1-z)^k z^{n-k} \sum_{i \in I} a_i R\left(M_C; q_1^{b_{i1}} \cdots q_s^{b_{is}} \frac{z}{1-z}, \frac{1-z}{z}\right).$$

The main import of Theorem 13 arises from its indication of the extent of what the matroid, and in particular its rank generating function, can say about the codes that represent it over given finite fields. Furthermore, Theorem 13 has broad applicability since it would seem reasonable to expect that, for a given invariant code structure family $\mathscr{S}$, the number $a(\mathscr{S}; q_1, \ldots, q_s, k)$ is a rational function in $q_1^k, \ldots, q_s^k$ and therefore is of the form $\sum_{i \in I} a_i \prod_{j=1}^{s} q_j^{b_{ij}k}$, where the coefficients a_i, b_{ij} are independent of k. To illustrate some special cases of Theorem 13 in which the s-tuple of linear codes consists merely of a single linear code $C \subseteq \mathbb{F}_q^E$, consider the following identities (see [1,17,24] for example),

$$\begin{aligned} (q^k)_m &= \sum_{i=0}^{m} s(m,i)(q^i)^k \\ \binom{q^k}{m} &= \sum_{i=0}^{m} \frac{s(m,i)}{m!}(q^i)^k \\ \binom{q^k+m-1}{m} &= \sum_{i=0}^{m} \frac{|s(m,i)|}{m!}(q^i)^k \\ \begin{bmatrix} k \\ r \end{bmatrix} &= \sum_{i=0}^{r} \frac{(-1)^{r-i}}{[r]_r} q^{\binom{r-i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} (q^i)^k, \end{aligned}$$

where the term $s(m,i)$ denotes a Stirling number of the first kind.

Corollaries 14–18 follow immediately from Theorem 13, Table 1, and the above identities.

Corollary 14. *If $\mathscr{S}$ is the family consisting of m-tuples of vectors, then*

$$A_C^{\mathscr{S}}(\mathbf{z}) = R_{1-x,x}(M_C; q^m, 1, \mathbf{z})$$

and

$$A_C^{\mathscr{S}}(z) = (1-z)^k z^{n-k} R\left(M_C; \frac{q^m z}{1-z}, \frac{1-z}{z}\right).$$

Corollary 14 was previously proved in [5] by the author.

Corollary 15. *If $\mathscr{S}$ is the family of all m-tuples of distinct vectors, then*

$$A_C^{\mathscr{S}}(\mathbf{z}) = \sum_{i=0}^{m} s(m,i) R_{1-x,x}(M_C; q^i, 1, \mathbf{z})$$

and

$$A_C^{\mathscr{S}}(z) = (1-z)^k z^{n-k} \sum_{i=0}^{m} s(m,i) R\left(M_C; \frac{q^i z}{1-z}, \frac{1-z}{z}\right).$$

Corollary 16. *If $\mathscr{S}$ is the code structure family consisting of unordered sets of m distinct vectors, then*

$$A_C^{\mathscr{S}}(\mathbf{z}) = \frac{1}{m!} \sum_{i=0}^{m} s(m,i) R_{1-x,x}(M_C; q^i, 1, \mathbf{z})$$

and

$$A_C^{\mathscr{S}}(z) = \frac{1}{m!}(1-z)^k z^{n-k} \sum_{i=0}^{m} s(m,i) R\left(M_C; \frac{q^i z}{1-z}, \frac{1-z}{z}\right).$$

Corollary 17. *If $\mathscr{S}$ is the code structure family consisting of unordered multisets of m vectors, then*

$$A_C^{\mathscr{S}}(\mathbf{z}) = \frac{1}{m!} \sum_{i=0}^{m} |s(m,i)| R_{1-x,x}(M_C; q^i, 1, \mathbf{z})$$

and

$$A_C^{\mathscr{S}}(z) = \frac{1}{m!}(1-z)^k z^{n-k} \sum_{i=0}^{m} |s(m,i)| R\left(M_C; \frac{q^i z}{1-z}, \frac{1-z}{z}\right).$$

Corollary 18. *If $\mathscr{S}$ is the code structure family consisting of r-dimensional subspaces, then*

$$A_C^{\mathscr{S}}(\mathbf{z}) = \frac{1}{[r]_r} \sum_{i=0}^{r} (-1)^{r-i} q^{\binom{r-i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} R_{1-x,x}(M_C; q^i, 1, \mathbf{z})$$

and

$$A_C^{\mathscr{S}}(z) = \frac{1}{[r]_r}(1-z)^k z^{n-k} \sum_{i=0}^{r} (-1)^{r-i} q^{\binom{r-i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} R\left(M_C; \frac{q^i z}{1-z}, \frac{1-z}{z}\right).$$

Corollary 18 extends Dowling [11, Theorem 2].

The two corollaries below conclude this section by describing two simple cases of Theorem 13 in which $\mathscr{S}$ is an invariant code structure family over the fields $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_s}$, and $C_1 \subseteq \mathbb{F}_{q_1}^E, \ldots, C_s \subseteq \mathbb{F}_{q_s}^E$ are k-dimensional linear codes with a common vector matroid $M = M_{C_1} = \cdots = M_{C_s}$. The corollaries follow immediately from Theorem 13 and Table 2.

Corollary 19. *If $\mathscr{S}$ is the code structure family consisting of ordered s-tuples $(T_1, \ldots, T_s)$ where $T_i \subseteq C_i$ is an ordered m_i-tuple $(i = 1, \ldots, s)$, then*

$$A_{\mathbf{C}}^{\mathscr{S}}(\mathbf{z}) = R_{1-x,x}(M; q_1^{m_1} \cdots q_s^{m_s}, 1, \mathbf{z})$$

and

$$A_{\mathbf{C}}^{\mathscr{S}}(z) = (1-z)^k z^{n-k} R\left(M; q_1^{m_1} \cdots q_s^{m_s} \frac{z}{1-z}, \frac{1-z}{z}\right).$$

Corollary 20. *If $\mathscr{S}$ is the code structure family consisting of vectors contained in the multiset $C_1 \cup \cdots \cup C_s$, then*

$$A_{\mathbf{C}}^{\mathscr{S}}(\mathbf{z}) = \sum_{i=1}^{s} R_{1-x,x}(M; q_i, 1, \mathbf{z})$$

and

$$A_{\mathbf{C}}^{\mathscr{S}}(z) = (1-z)^k z^{n-k} \sum_{i=1}^{s} R\left(M; \frac{q_i z}{1-z}, \frac{1-z}{z}\right).$$

5. MacWilliams-type identities

As an application of Theorem 3, Greene [13] presented a simple proof of the following identity due to MacWilliams (see [18,19]) that relates the weight enumerator of a linear code to that of its dual. Throughout the whole of this section, let $C \subseteq \mathbb{F}_q^E$ be a k-dimensional linear code.

Theorem 21 (*MacWilliams identity*). *If $A(z)$ and $B(z)$ denote the weight enumerators of the code C and its dual $C^\perp$, then*

$$B(z) = \frac{1}{q^k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right).$$

By generalising Theorem 3, Greene's procedure has been repeated by Barg [4] and the author [5] in order to obtain generalisations of the MacWilliams identity. Similarly, Greene's

procedure is repeated in the present section by using the results of Section 4 to prove a general form of the MacWilliams identity (Theorem 22) and thereby a number of explicit generalisations. For a sample of the many alternative ways in which the MacWilliams identity has previously been generalised, see [14,19,20,31].

In Theorem 22,

- $\mathscr{E}$ denotes the family of enumerators of codes with respect to given invariant code structure families;
- $\{\mathscr{S}_i\}_I$ and $\{\mathscr{T}_j\}_J$ are sets of invariant code structure families over $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_s}$;
- $C_1 \subseteq \mathbb{F}_{q_1}^E, \ldots, C_s \subseteq \mathbb{F}_{q_s}^E$ are k-dimensional linear codes with a common vector matroid $M = M_{C_1} = \cdots = M_{C_s}$; and
- $\mathscr{S}$ is the code structure family consisting of ordered s-tuples $(T_1, \ldots, T_s)$ where each $T_i \subseteq C_i$ is an ordered m_i-tuple $(i = 1, \ldots, s)$.

Define $\mathbf{C} = (C_1, \ldots, C_s)$, $\mathbf{C}^\perp = (C_1^\perp, \ldots, C_s^\perp)$, and $\tilde{q} = q_1^{m_1} \cdots q_s^{m_s}$.

Theorem 22. *If $f : \mathscr{E}^I \mapsto \mathscr{E}$ and $g : \mathscr{E}^J \mapsto \mathscr{E}$ are maps for which it holds that $f(\{A_{\mathbf{C}}^{\mathscr{S}_i}(\mathbf{z})\}_I) = A_{\mathbf{C}}^{\mathscr{S}}(\mathbf{z})$ and $g(\{A_{\mathbf{C}^\perp}^{\mathscr{T}_j}(\mathbf{z})\}_J) = A_{\mathbf{C}^\perp}^{\mathscr{S}}(\mathbf{z})$, then*

$$g(\{A_{\mathbf{C}^\perp}^{\mathscr{T}_j}(\mathbf{z})\}_J) = \frac{1}{\tilde{q}^k}\left(\prod_{e\in E}(1+(\tilde{q}-1)z_e)\right) f\left(\left\{A_{\mathbf{C}}^{\mathscr{S}_i}\left(\left\{\frac{1-z_e}{1+(\tilde{q}-1)z_e}\right\}_E\right)\right\}_I\right)$$

and

$$g(\{A_{\mathbf{C}^\perp}^{\mathscr{T}_j}(z)\}_J) = \frac{1}{\tilde{q}^k}(1+(\tilde{q}-1)z)^n f\left(\left\{A_{\mathbf{C}}^{\mathscr{S}_i}\left(\frac{1-z}{1+(\tilde{q}-1)z}\right)\right\}_I\right).$$

Proof. The proof is by straightforward computation. By Corollary 19,

$$g(\{A_{\mathbf{C}^\perp}^{\mathscr{T}_j}(\mathbf{z})\}_J) = A_{\mathbf{C}^\perp}^{\mathscr{S}}(\mathbf{z}) = R_{1-x,x}(M^*; \tilde{q}, 1, \mathbf{z}).$$

If follows from Proposition 4 that $g(\{A_{\mathbf{C}^\perp}^{\mathscr{T}_j}(\mathbf{z})\}_J) = R_{x,1-x}(M; 1, \tilde{q}, \mathbf{z})$. Hence,

$$\begin{aligned} g(\{A_{\mathbf{C}^\perp}^{\mathscr{T}_j}(\mathbf{z})\}_J) &= \sum_{X\subseteq E} \tilde{q}^{|X|-\rho(X)}\left(\prod_{e\in X} z_e\right)\prod_{f\in E-X}(1-z_e) \\ &= \frac{1}{\tilde{q}^k}\sum_{X\subseteq E} \tilde{q}^{\rho(E)-\rho(X)}\left(\prod_{e\in X}\tilde{q}z_e\right)\prod_{f\in E-X}(1-z_e) \\ &= \frac{1}{\tilde{q}^k}\left(\prod_{e\in E}(1+(\tilde{q}-1)z_e)\right) R_{1-x,x}\left(M; \tilde{q}, 1, \left\{\frac{1-z_e}{1+(\tilde{q}-1)z_e}\right\}_E\right). \end{aligned}$$

By Corollary 19,

$$g(\{A^{\mathscr{T}^j}_{\mathbf{C}^\perp}(\mathbf{z})\}_J) = \frac{1}{\tilde{q}^k}\left(\prod_{e\in E}(1+(\tilde{q}-1)z_e)\right) A^{\mathscr{S}}_{\mathbf{C}}\left(\left\{\frac{1-z_e}{1+(\tilde{q}-1)z_e}\right\}_E\right)$$
$$= \frac{1}{\tilde{q}^k}\left(\prod_{e\in E}(1+(\tilde{q}-1)z_e)\right) f\left(\left\{A^{\mathscr{S}^i}_{\mathbf{C}}\left(\left\{\frac{1-z_e}{1+(\tilde{q}-1)z_e}\right\}_E\right)\right\}_I\right).$$

The second identity follows by setting $z_e = z$ for all $e \in E$. □

For each $X \subseteq E$, let the coefficients $a^{\mathscr{S}}_X$ and $b^{\mathscr{S}}_X$ be defined by the expansions

$$f(\{A^{\mathscr{S}^i}_{\mathbf{C}}(\mathbf{z})\}_I) = \sum_{X\subseteq E} a^{\mathscr{S}}_X \prod_{e\in X} z_e \quad \text{and} \quad g(\{A^{\mathscr{T}^j}_{\mathbf{C}^\perp}(\mathbf{z})\}_J) = \sum_{X\subseteq E} b^{\mathscr{S}}_X \prod_{e\in X} z_e.$$

Corollary 23. *If $X \subseteq E$, then*

$$\sum_{Y\subseteq X} b^{\mathscr{S}}_Y = \tilde{q}^{|X|-k} \sum_{Y\subseteq E-X} a^{\mathscr{S}}_Y.$$

Proof. Set $z_e = 1$ for each element $e \in X$ and $z_e = 0$ for each element $e \in E - X$. Now apply Theorem 22. □

To illustrate the application of Theorem 22, consider Corollaries 24–28 in all of which the functions f and g have been chosen to be identical. These corollaries follow directly from Theorem 22, Table 1, and the observation that $(q^m)^k$ may be expanded as

$$(q^m)^k = \sum_{j=0}^{m} S(m,j)(q^k)_j,$$
$$(q^m)^k = \sum_{j=0}^{m} j!S(m,j)\binom{q^k}{j},$$
$$(q^m)^k = \sum_{j=0}^{m} (-1)^{m-j} j!S(m,j)\binom{q^k+j-1}{j}$$

and

$$(q^m)^k = \sum_{r=0}^{m} [m]_r \begin{bmatrix} k \\ r \end{bmatrix},$$

where $S(m,j)$ is a Stirling number of the second kind (see [1,17,24]). For simplicity, the remaining parts of this section concern only code structure families over a single linear code $C \subseteq \mathbb{F}_q^E$.

Corollary 24. *If $\mathscr{S}$ is the code structure family consisting of m-tuples of vectors, then*

$$A^{\mathscr{S}}_{C^\perp}(\mathbf{z}) = \frac{1}{q^{km}}\left(\prod_{e\in E}(1+(q^m-1)z_e)\right)A^{\mathscr{S}}_C\left(\left\{\frac{1-z_e}{1+(q^m-1)z_e}\right\}_E\right)$$

and

$$A^{\mathscr{S}}_{C^\perp}(z) = \frac{1}{q^{km}}(1+(q^m-1)z)^n A^{\mathscr{S}}_C\left(\frac{1-z}{1+(q^m-1)z}\right).$$

The first identity in Corollary 24 has been proven for the case $m=1$ by Simonis [23]. The second identity in Corollary 24 was initially discovered and proved by Shiromoto [22]. The whole corollary is also proved in [5].

Corollary 25. *If $\mathscr{S}_j$ is the code structure family consisting of j-tuples of distinct vectors, then for all $m \geqslant 0$,*

$$\sum_{j=0}^{m} S(m,j)A^{\mathscr{S}_j}_{C^\perp}(\mathbf{z}) = \frac{1}{q^{km}}\left(\prod_{e\in E}(1+(q^m-1)z_e)\right)\sum_{j=0}^{m} S(m,j)A^{\mathscr{S}_j}_{C}\left(\left\{\frac{1-z_e}{1+(q^m-1)z_e}\right\}_E\right)$$

and

$$\sum_{j=0}^{m} S(m,j)A^{\mathscr{S}_j}_{C^\perp}(z) = \frac{1}{q^{km}}(1+(q^m-1)z)^n\sum_{j=0}^{m} S(m,j)A^{\mathscr{S}_j}_{C}\left(\frac{1-z}{1+(q^m-1)z}\right).$$

Corollary 26. *Let $\mathscr{S}_j$ be the code structure family consisting of unordered sets of j distinct vectors. Then for all $m \geqslant 0$,*

$$\sum_{j=0}^{m} j!S(m,j)A^{\mathscr{S}_j}_{C^\perp}(\mathbf{z}) = \frac{1}{q^{km}}\left(\prod_{e\in E}(1+(q^m-1)z_e)\right)\sum_{j=0}^{m} j!S(m,j)A^{\mathscr{S}_j}_{C}\left(\left\{\frac{1-z_e}{1+(q^m-1)z_e}\right\}_E\right)$$

and

$$\sum_{j=0}^{m} j!S(m,j)A^{\mathscr{S}_j}_{C^\perp}(z) = \frac{1}{q^{km}}(1+(q^m-1)z)^n \times\sum_{j=0}^{m} j!S(m,j)A^{\mathscr{S}_j}_{C}\left(\frac{1-z}{1+(q^m-1)z}\right).$$

Corollary 27. *Let $\mathscr{S}_j$ be the code structure family consisting of all unordered multisets of j vectors. Then for all $m \geqslant 0$,*

$$\sum_{j=0}^{m}(-1)^{m-j}\, j!S(m,\, j)A_{C^\perp}^{\mathscr{S}_j}(\mathbf{z}) = \frac{1}{q^{km}}\left(\prod_{e\in E}(1+(q^m-1)z_e)\right) \times \sum_{j=0}^{m}(-1)^{m-j}\, j!S(m,\, j)A_{C}^{\mathscr{S}_j}\left(\left\{\frac{1-z_e}{1+(q^m-1)z_e}\right\}_E\right)$$

and

$$\sum_{j=0}^{m}(-1)^{m-j}\, j!S(m,\, j)A_{C^\perp}^{\mathscr{S}_j}(z) = \frac{1}{q^{km}}(1+(q^m-1)z)^n \sum_{j=0}^{m}(-1)^{m-j}\, j!S(m,\, j)A_{C}^{\mathscr{S}_j}\left(\frac{1-z}{1+(q^m-1)z}\right).$$

Corollary 28. *Suppose that $\mathscr{S}_r$ is the code structure family consisting of all r-dimensional subspaces. Then for all $m \geqslant 0$,*

$$\sum_{r=0}^{m}[m]_r A_{C^\perp}^{\mathscr{S}_r}(\mathbf{z}) = \frac{1}{q^{km}}\left(\prod_{e\in E}(1+(q^m-1)z_e)\right)\sum_{r=0}^{m}[m]_r A_{C}^{\mathscr{S}_r}\left(\left\{\frac{1-z_e}{1+(q^m-1)z_e}\right\}_E\right)$$

and

$$\sum_{r=0}^{m}[m]_r A_{C^\perp}^{\mathscr{S}_r}(z) = \frac{1}{q^{km}}(1+(q^m-1)z)^n \sum_{r=0}^{m}[m]_r A_{C}^{\mathscr{S}_r}\left(\frac{1-z}{1+(q^m-1)z}\right).$$

The results of Corollary 28 also appear in [5]. The second identity in Corollary 28 was initially discovered and proved by Kløve [15]. A matroid proof was later provided by Barg [4].

Corollaries 24–28 each illustrate Theorem 22 with respect to one code structure family. Broader possibilities arise, however, if two or more distinct code structure families are chosen. For instance, if two distinct code structure families are chosen from the five code structure families in Corollaries 24–28, then we obtain $\binom{5}{2} = 10$ distinct generalisations of the MacWilliams identity. Of these, we will only state the following result.

Corollary 29. *Let $\mathscr{S}_j$ and $\mathscr{T}_r$ be the code structure families consisting of all unordered multisets of j vectors, and of r-dimensional subspaces, respectively. Then for all $m \geqslant 0$,*

$$\sum_{j=0}^{m} (-1)^{m-j} j! S(m, j) A_{C^\perp}^{\mathscr{S}_j}(\mathbf{z}) = \frac{1}{q^{km}} \left(\prod_{e \in E} (1 + (q^m - 1) z_e) \right) \sum_{r=0}^{m} [m]_r A_C^{\mathscr{T}_r} \left(\left\{ \frac{1 - z_e}{1 + (q^m - 1) z_e} \right\}_E \right)$$

and

$$\sum_{j=0}^{m} (-1)^{m-j} j! S(m, j) A_{C^\perp}^{\mathscr{S}_j}(z) = \frac{1}{q^{km}} (1 + (q^m - 1) z)^n \times \sum_{r=0}^{m} [m]_r A_C^{\mathscr{T}_r} \left(\frac{1 - z}{1 + (q^m - 1) z} \right).$$

To conclude this section, let us derive a general Delsarte–MacWilliams type bound. Let $\{\mathscr{S}_i\}_I$ and $\{\mathscr{T}_j\}_J$ be sets of invariant code structure families over the fields $\mathbb{F}_{q_1}, \ldots, \mathbb{F}_{q_s}$, let $C_1 \subseteq \mathbb{F}_{q_1}^E, \ldots, C_s \subseteq \mathbb{F}_{q_s}^E$ be k-dimensional linear codes with a common vector matroid $M = M_{C_1} = \cdots = M_{C_s}$, and let $\mathscr{S}$ be the code structure family consisting of ordered s-tuples $(T_1, \ldots, T_s)$ where each $T_i \subseteq C_i$ is an ordered m_i-tuple ($i = 1, \ldots, s$). If $f : \mathscr{E}^I \mapsto \mathscr{E}$ and $g : \mathscr{E}^J \mapsto \mathscr{E}$ are maps such that $f(\{A_{\mathbf{C}}^{\mathscr{S}_i}(\mathbf{z})\}_I) = A_{\mathbf{C}}^{\mathscr{S}}(\mathbf{z})$ and $g(\{A_{\mathbf{C}^\perp}^{\mathscr{T}_j}(\mathbf{z})\}_J) = A_{\mathbf{C}^\perp}^{\mathscr{S}}(\mathbf{z})$, then let the coefficients $a_i^{\mathscr{S}}$ and $b_i^{\mathscr{S}}$ ($i = 0, \ldots, n$) be defined by the expansions

$$f(\{A_{\mathbf{C}}^{\mathscr{S}_i}(z)\}_I) = \sum_{i=0}^{n} a_i^{\mathscr{S}} z^i \quad \text{and} \quad g(\{A_{\mathbf{C}^\perp}^{\mathscr{T}_j}(z)\}_J) = \sum_{i=0}^{n} b_i^{\mathscr{S}} z^i.$$

The following theorem is a consequence of Theorem 22.

Theorem 30. *Let $\mathbf{a}^{\mathscr{S}} = (a_0^{\mathscr{S}}, \ldots, a_n^{\mathscr{S}})$ and $\mathbf{b}^{\mathscr{S}} = (b_0^{\mathscr{S}}, \ldots, b_n^{\mathscr{S}})$. Then*

$$\tilde{q}^k \mathbf{b}^{\mathscr{S}} = \mathbf{a}^{\mathscr{S}} \mathbf{P},$$

where $\tilde{q} = q_1^{m_1} \cdots q_s^{m_s}$ and $\mathbf{P} = (p_{ij})$ is an $(n+1) \times (n+1)$ Krawtchouk matrix with entries $p_{ij} = \sum_{l=0}^{n} (-1)^l \binom{i}{l} \binom{n-i}{j-l} (\tilde{q} - 1)^{j-l}$.

Since the coefficients b_i are non-negative integers, Theorem 30 has as a corollary the following Delsarte–MacWilliams type bound.

Corollary 31. *For each integer $j = 0, \ldots, n$, $\sum_{i=0}^{n} p_{ij} a_i^{\mathscr{S}} \geqslant 0$. Indeed, this sum is a non-negative integer that is divisible by $\tilde{q}^k$.*

6. Concluding remarks

The corollaries that illustrate the application of Theorem 13 and 22 demonstrate but a few of the many ways in which these theorems may be applied. A large class of such ways arise from the code structure families $\mathscr{S}$ over $\mathbb{F}_q$ for which the sequence $(a(\mathscr{S}; q, k))_{k\geqslant 0}$ forms a basis of polynomials (in the variable $x = q$ or in the variable $x = q^m$). The examples appearing in the corollaries of the previous sections all belong to this class since each of the polynomials

$$q^{km},\ (q^k)_m,\ \binom{q^k}{m},\ \binom{q^k+m-1}{m} \quad \text{and} \quad \begin{bmatrix} k \\ r \end{bmatrix}$$

generates a sequence for $k = 0, 1, \ldots$ that is a polynomial basis. Thus, the identities on page 12 and 15 are merely change of basis identities; indeed, the two sets of identities are mutually inverse. Furthermore, Corollaries 14–18 and Corollaries 24–28 are equivalent, respectively. By finding other code structure families $\mathscr{S}$ for which the sequence $(a(\mathscr{S}; q, k))_{k\geqslant 0}$ forms a basis of polynomials, we are able to obtain further equivalent results.

A collection of code structure families may be accorded an analogue of Theorem 3 or a MacWilliams-type identity even when the associated sequence of polynomials does not form a polynomial basis. To illustrate this, consider the following somewhat trivial example. Let $\mathscr{S}_0$, $\mathscr{S}_1$, and $\mathscr{S}_2$ be the structure families over $\mathbb{F}_q$ consisting of zero vectors, non-zero vectors, and all vectors, respectively. Then

$$a(\mathscr{S}_0; q, k) = 1, \quad a(\mathscr{S}_1; q, k) = q^k - 1 \quad \text{and} \quad a(\mathscr{S}_2; q, k) = q^k,$$

so $\frac{1}{2}a(\mathscr{S}_0; q, k) + \frac{1}{2}a(\mathscr{S}_1; q, k) + \frac{1}{2}a(\mathscr{S}_2; q, k) = q^k$. Theorem 22 therefore provides us with the following MacWilliams-type identities

$$\sum_{j=0,1,2} \frac{1}{2} A_{C^\perp}^{\mathscr{S}_j}(\mathbf{z}) = \frac{1}{q^k} \left(\prod_{e\in E} (1+(q-1)z_e) \right) \sum_{j=0,1,2} \frac{1}{2} A_C^{\mathscr{S}_j} \left(\left\{ \frac{1-z_e}{1+(q-1)z_e} \right\}_E \right)$$

and

$$\sum_{j=0,1,2} \frac{1}{2} A_{C^\perp}^{\mathscr{S}_j}(z) = \frac{1}{q^k} (1+(q-1)z)^n \sum_{j=0,1,2} \frac{1}{2} A_C^{\mathscr{S}_j} \left(\frac{1-z}{1+(q-1)z} \right),$$

in spite of the fact that the set $\{1, q^k - 1, q^k\}$ is clearly not contained in any polynomial basis.

Acknowledgements

I gratefully thank Peter Cameron, Rikke Bundgaard-Nielsen, and an anonymous referee for their valuable suggestions and advice.

References

[1] M. Aigner, Combinatorial Theory, Springer, New York, 1979.
[2] A.E. Ashikhmin, A. Barg, Minimal vectors in linear codes, IEEE Trans. Inform. Theory 44 (1998) 2010–2017.

[3] C.A. Athanasiadis, Characteristic polynomials of subspace arrangements and finite fields, Adv. Math. 122 (1996) 193–233.
[4] A. Barg, The matroid of supports of a linear code, Appl. Algebra Engrg. Comm. Comput. 8 (1997) 165–172.
[5] T. Britz, MacWilliams identities and matroid polynomials, Electron. J. Combin. 9 (2002) R19.
[6] T. Britz, Higher support matroids, submitted for publication.
[7] T. Britz, C.G. Rutherford, Covering radii are not matroid invariants, Discrete Math. 296 (2005) 117–120.
[8] R.A. Brualdi, V.S. Pless, J.S. Beissinger, On the MacWilliams identities for linear codes, Linear Algebra Appl. 107 (1988) 181–189.
[9] T. Brylawski, Appendix of matroid cryptomorphisms, in: Theory of Matroids, Cambridge University Press, Cambridge-New York, 1986, pp. 298–312.
[10] H. Crapo, G.-C. Rota, On the Foundations of Combinatorial Theory: Combinatorial Geometries, MIT Press, Cambridge, MA, London, 1970 (Preliminary Edition).
[11] T.A. Dowling, Codes, packings and the critical problem, in: Applicazioni University of Perugia, Perugia, 1970, pp. 209–224. (Ist. Mat., University of Perugia, Perugia, 1971).
[12] S.D. Fisher, M.N. Alexander, Matrices over a finite field, Amer. Math. Monthly 73 (1966) 639–641.
[13] C. Greene, Weight enumeration and the geometry of linear codes, Stud. Appl. Math. 55 (1976) 119–128.
[14] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40 (1994) 301–319.
[15] T. Kløve, Support weight distribution of linear codes, Discrete Math. 106/107 (1992) 311–316.
[16] J. Kung, Critical problems, in: Matroid Theory, Seattle, WA, 1995, Contemporary Mathematics, vol. 197, American Mathematical Society, Providence, RI, 1996, pp. 1–127.
[17] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, Cambridge University Press, Cambridge, 1992.
[18] F.J. MacWilliams, A theorem on the distribution of weights in a systematic code, Bell System Tech. J. 42 (1963) 79–94.
[19] F.J. MacWilliams, N.J. Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing Company, Amsterdam, 1978.
[20] F.J. MacWilliams, N.J. Sloane, J.-M. Goethals, The MacWilliams identities for nonlinear codes, Bell System Tech. J. 51 (1972) 803–819.
[21] J. Oxley, Matroid Theory, Oxford University Press, New York, 1992.
[22] K. Shiromoto, The weight enumerator of linear codes over $GF(q^m)$ having generator matrix over $GF(q)$, Des. Codes Cryptogr. 16 (1999) 87–92.
[23] J. Simonis, MacWilliams identities and coordinate partitions, Linear Algebra Appl. 216 (1995) 81–91.
[24] R.P. Stanley, Enumerative Combinatorics, vol. 1, Cambridge University Press, Cambridge, New York, 1997.
[25] L. Traldi, Series and parallel reductions for the Tutte polynomial, Discrete Math. 220 (2000) 291–297.
[26] L. Traldi, Chain polynomials and Tutte polynomials, Discrete Math. 248 (2002) 279–282.
[27] W.T. Tutte, A homotopy theorem for matroids. II, Trans. Amer. Math. Soc. 88 (1958) 161–174.
[28] W.T. Tutte, Lectures on matroids, J. Res. Natl. Bur. Standards, Sect. B 69 (1965) 1–47.
[29] D.J.A. Welsh, Matroid Theory, Academic Press, London, 1976.
[30] H. Whitney, On the abstract properties of linear dependence, Amer. J. Math. 57 (1935) 509–533.
[31] T. Yoshida, MacWilliams identities for linear codes with group action, Kumamoto J. Math. 6 (1993) 29–45.
[32] T. Zaslavsky, Strong Tutte functions of matroids and graphs, Trans. Amer. Math. Soc. 334 (1992) 317–347.